

Research Article

System for Malicious Node Detection in IPv6-Based Wireless Sensor Networks

Kresimir Grgic, Drago Zagar, and Visnja Krizanovic Cik

Faculty of Electrical Engineering, Josip Juraj Strossmayer University of Osijek, Kneza Trpimira 2b, 31000 Osijek, Croatia

Correspondence should be addressed to Kresimir Grgic; kresimir.grgic@etfos.hr

Received 24 March 2016; Accepted 15 June 2016

Academic Editor: Fei Yu

Copyright © 2016 Kresimir Grgic et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The trend of implementing the IPv6 into wireless sensor networks (WSNs) has recently occurred as a consequence of a tendency of their integration with other types of IP-based networks. The paper deals with the security aspects of these IPv6-based WSNs. A brief analysis of security threats and attacks which are present in the IPv6-based WSN is given. The solution to an adaptive distributed system for malicious node detection in the IPv6-based WSN is proposed. The proposed intrusion detection system is based on distributed algorithms and a collective decision-making process. It introduces an innovative concept of probability estimation for malicious behaviour of sensor nodes. The proposed system is implemented and tested through several different scenarios in three different network topologies. Finally, the performed analysis showed that the proposed system is energy efficient and has a good capability to detect malicious nodes.

1. Introduction

Numerous intelligent sensors with basic computational and wireless communication capabilities are currently embedded into various devices and instruments worldwide. Since their number is growing rapidly, it could be expected that wireless sensor nodes will vastly outnumber conventional computers and other networked devices in the near future. Wireless sensor networks (WSNs) were the subject of intensive research and development during the last decade [1–3]. Due to strict resource constraints (both power and computational) the implementation of conventional Internet protocol architecture in WSNs used to be avoided at first, resulting in numerous noninteroperable solutions. Further development of WSNs naturally led to efforts to interconnect and integrate a WSN with conventional IP networks. These efforts resulted in certain frameworks and adaptation standards that enable the use of the IP in a WSN environment.

At the same time, a conventional IP network has also evolved and currently passes through the gradual implementation of the IPv6 (Internet Protocol version 6) that should replace the IPv4 in the future [4]. Current technologies of the WSN and IPv6 are highly complementary, and many efforts are currently focused on convergence of IPv6 and low power

multihop WSNs. The integration of sensor networks with IP networks will significantly diversify their array of applications. Certainly, it is possible to realize such integration efficiently and transparently for the end user, but there still remain some problems that require novel adequate solutions or optimization of existing solutions. Seamless integration of sensor networks with IP networks that satisfies demands on flexibility, scalability, and robustness represents the most important foundation for the Internet of Things (IoT) concept [5]. Thereby, the accent is on the implementation of the IPv6, since it provides huge address space and autoconfiguration mechanisms and extensibility (to support future innovations).

Very important aspects of the Internet of Things are security issues and their adequate solutions [6]. Solutions to security issues are an important precondition for wider acceptance and use of integrated sensor networks with IP networks. The implementation of the IPv6 into WSNs brings some specificities that hamper the use of existing security solutions known from IPv6 networks and conventional sensor networks. It is necessary to thoroughly adapt existing solutions and to invent novel solutions for the implementation in IPv6-based sensor networks. Node compromise and malicious behaviour make a quite possible scenario,

especially in networks with a large number of nodes, such as sensor networks.

The lack of quality, effective, and energy efficient intrusion detection system for IPv6-based WSN was the strongest motivation for the authors to focus the research efforts into this area. Existing proposals of intrusion detection systems for WSNs are focused on conventional WSNs, without taking care of certain specificities of IPv6-based WSNs. The fact that IPv6-based WSNs (being the basis of the Internet of Things) may possibly include a very large number of nodes motivated the authors to focus their research on distributed system based on cooperative algorithms and collective decision-making. Diversity of possible applications of IPv6-based WSNs was a motive to develop adaptive system suitable for different application requirements.

Therefore, this paper proposes a system for detecting malicious nodes in an IPv6-based WSN. The proposed system is designed for the IPv6 environment and it supports the IPv6 stack in a WSN. It is implemented into the sensor network that uses the IEEE 802.15.4 standard and the 6LoWPAN adaptation layer. For routing purposes, the RPL (routing protocol for low power and lossy networks) was implemented as the first routing protocol for sensor networks with full support for the IPv6. The UDP (user datagram protocol) is used as the transport layer protocol. The system for malicious node detection is implemented at the application layer. The proposed system uses cooperative algorithms and a collective decision-making procedure, so it is fully distributed and adaptive. Besides node characterization as malicious or legitimate, the system also estimates a probability of malicious behaviour for suspected nodes. The paper presents the implementation of the IPv6 stack into the WSN. Furthermore, the descriptions of the proposed intrusion detection system and its implementation are also given. The system is implemented in different characteristic scenarios, and the obtained results are analysed. Finally, some conclusions are drawn and some suggestions for future development are outlined.

2. IPv6 in Wireless Sensor Networks

The development of the IPv6 started in 1995, when it was obvious that some problems with the IPv4 will become more emphasised in the future (e.g., address space exhaustion, security issues, complex configuration, and routing table enlargement). Compared with IPv4, the IPv6 brings some significant improvements, such as 128-bit address space, a fixed-length simplified header, autoconfiguration mechanisms, and security improvements. Currently, the transition from IPv4 to the IPv6 is a long-lasting ongoing process [7].

Wireless sensor networks (WSNs) represent a special subgroup of mobile ad hoc networks (MANETs). However, strong computational and power limitations make them in some aspects significantly different from conventional MANETs. A WSN consists of a large number of inexpensive sensor nodes capable of sensing, basic data processing, and wireless communication with other nodes. WSN functions are based on communication between nodes and collaborative algorithms. Unfortunately, due to the above-mentioned limitations, most of existing technical and algorithmic solu-

tions known from MANETs cannot be directly applied to the WSN. Therefore, the WSN required adaptations of existing solutions and development of novel ones. Strict demands for low costs, small node dimensions, and energy efficiency noticeably influence the design of networking protocols and algorithms. They are designed with focus on consumption minimisation to prolong network lifetime. Since sensor nodes may be equipped with many different types of sensors, wireless sensor networks have a large variety of possible applications [8]. Sensor nodes with adequate sensors can be used for both continuous monitoring of the observed phenomenon and detection of certain events. In addition to detection, they can also identify the event that occurred and designate its location. Also, sensor nodes can be locally connected with different types of actuators. Today, WSNs are used for various military, environmental, health, home, and industrial applications.

In the beginning of WSN development, the implementation of the omnipresent and generally accepted IP stack into the WSN was considered impractical and inadequate. The IP was considered too demanding to operate properly with strongly limited resources. Therefore, the WSN usually used some alternative solutions (different protocols developed specially for WSNs) and avoided the IP. Unfortunately, a variety of protocols and the absence of a unique standard limited connectivity and interoperability of sensor networks with other types of networks. Consequently, during the last few years many efforts were focused on the implementation of the IP into the WSN, with necessary adaptations [9–11]. Since traditional IP networks are in transition from IPv4 to the IPv6, focus is on the implementation of the IPv6 into WSN.

The IETF working group 6LoWPAN (IPv6 over Low power Wireless Personal Area Network) defined the necessary adaptation layer that enables the implementation of the IPv6 into the WSN protocol stack. The adaptation is indispensable since the frame size used on the WSN physical layer is usually much smaller than that in conventional IP networks. The dominant standard for the physical layer in WSNs is currently IEEE 802.15.4. Therefore, the 6LoWPAN adaptation layer enables adaptation of an IPv6 packet for transmission within the IEEE 802.15.4 frame. The 6LoWPAN adaptation layer defines frame format, forming methods for link-local addresses and address autoconfiguration methods in networks based on IEEE 802.15.4. Additional specifications include methods for IPv6 header compression because of easier transfer over IEEE 802.15.4 links and resource savings. Although the IEEE 802.15.4 standard defines four types of frames (beacon frames, MAC command frames, acknowledgement frames, and data frames), IPv6 packets can be transferred only within data frames. Optionally, acknowledgements for received packets can be used.

A full IPv6 packet is too large for the IEEE 802.15.4 frame which has 127 bytes on the physical layer. Without any compression methods (maximal overhead) and with AES (advanced encryption standard) used on the data link layer, it would leave only 33 bytes available for the application layer data. Clearly, fragmentation would be necessary for larger data transfer. Since the fragmentation process consumes

additional resources, the 6LoWPAN adaptation layer focuses on header compression possibilities to get packets that could in most cases fit into the IEEE 802.15.4 frame. 6LoWPAN also defines compression of the UDP header and in the best case (local unicast communication) the UDP and IPv6 header can be compressed into 6 bytes.

The IETF working group ROLL (Routing Over Low power and Lossy networks) specified a new RPL (where wireless sensor networks also belong). The RPL is the first routing protocol with IPv6 support suitable for sensor networks. It was designed as a modular protocol, with a mandatory core part and optional application-depending features. It was used as a routing protocol for an IPv6-based WSN in all analysed scenarios [12].

3. Security Aspects of Wireless Sensor Networks

Security issues in wireless networks are more challenging than in wired networks due to the open nature of the communication medium. Therefore, it is often more difficult to secure MANETs compared to conventional wired networks. Although WSNs are a special subset of MANETs, their strong resource limitations bring additional difficulties in their security aspects. Since most of wireless networks also use the TCP/IP stack, most of security threats known from wired networks persist in wireless networks [13, 14]. Further, a wireless environment brings some new security threats unknown in wired networks. There are some differences between the WSN and MANET that disable a direct implementation of known MANET security mechanisms into the WSN: the WSN may have a significantly larger number of nodes that are more densely deployed, sensor nodes are prone to failures (due to environmental effects and limited power supply) and have stronger resource limitations than a typical MANET node, and WSNs usually use a broadcast communication paradigm, while point-to-point communication still dominates in MANETs [15–19].

Specified differences make WSNs more vulnerable to denial-of-service attacks. Also, well-known public key cryptography methods are still practically inapplicable in WSNs because of their computational demands. Development of quality key management mechanisms, secure routing protocols, secure data aggregation mechanisms, and intrusion detection mechanisms still represents a great challenge in WSNs, especially in an IPv6-based WSN.

Providing physical security of every sensor node in the WSN would require significant costs, which would also be contrary to the WSN concept as a network of cheap network nodes. Therefore, in most cases WSNs are considered to be prone to physical attacks, and research is focused on different methods for detection and prevention of different possible attack types where the attacker does not have any physical contact with sensor nodes or the base station.

A large variety of possible attack types can be classified according to different criterions. The attacks on the WSN can be divided into outsider attacks (originated from nodes that do not belong to the targeted network) and insider attacks (former legitimate nodes are compromised and start

with malicious behaviour) [20]. Also, attacks can be passive (eavesdropping and tracking of transferred data) or active (include certain modifications of existing dataflows and creating of new data intentionally by the attacker). The attacks on the sensor network can be focused on confidentiality and authentication, network availability (denial-of-service attacks), or data and service integrity.

The attacks focused on the physical layer are jamming and tampering. The attacker can use their transmitter to cause interference intentionally on WSN operational frequencies. Advanced methods for interference avoidance (like FHSS communication) increase sensor node complexity and raise their cost and energy consumption. Since in most WSNs communication is limited to only one channel, they are usually very vulnerable to jamming attacks. Also, in most cases sensor nodes are not physically protected, so they are exposed to tampering. Therefore, all security mechanisms for WSNs have to predict possible compromise of certain nodes and to implement a mechanism for their exclusion from the network [21].

If two or more nodes try to transmit at the same frequency, the collision will occur, causing packet loss. The attacker may intentionally cause collisions, most frequently during transmissions of acknowledgements. It is not difficult to detect such attack type, but it is very difficult to protect against them. If collision occurs, nodes continuously try to retransmit the packets, which may result in resource exhaustion [22, 23]. Resource exhaustion by retransmission can be reduced by limiting the frequency of medium access (on the MAC layer) and by using time-division multiplexing.

Some attacks on sensor networks focus on a routing mechanism, where the attacker spoofs or modifies routing information. In this way, the intruder can intentionally create routing loops, attract or reject network traffic, change existing routes, increase latency, and generate false error messages [24]. Some of these problems can be reduced or avoided by using message authentication codes and timestamps. Most WSNs use the multihop communication principle, assuming that every sensor node will act as a router and forward packets toward their destination. The malicious node can intentionally drop some packets and disable their further propagation. The easiest case to detect is when the intruder drops all incoming packets and refuses to forward them to their neighbours (a “black hole” attack). It is more difficult to detect the case when the attacker forwards packets selectively (a selective forwarding attack). A possible countermeasure is the use of multiple routes. The attacker can also falsify routing data (e.g., advertising quality route to the base station) in order to attract all traffic from a certain network part (a sinkhole attack). A sinkhole attack can be prevented by using exact geographic location data in the routing procedure [25, 26].

The attacker frequently uses hardware that is much more powerful than the average sensor node (e.g., a notebook computer). In that case, the attacker can use several false identities at the same time, when they introduce themselves as several legitimate nodes (a Sybil attack). A Sybil attack may have a significant impact on the data aggregation process and other distributed networking mechanisms (e.g., distributed data storage or an intrusion detection system). Possible

measures to prevent Sybil attacks must include a node identity validation mechanism [27]. If the attacker has two notebook computers, they can create a low-latency fast link between two distant network parts that is invisible for legitimate nodes (a wormhole attack). Possible countermeasures include precise temporal or geographical marking of every packet (which assumes precise network time synchronisation and exact location data) [28].

Attacks targeted at transport layer protocols usually misuse the connection establishment mechanism. The attacker repeatedly sends requests to connect in order to exhaust resources required for connection establishment. In that case, legitimate connection requests will be ignored due to lack of required resources. Also, some security threats in WSNs target directly the application layer, when the attacker tries to excessively stimulate sensors causing intensive data transfer that exhaust network resources (an overwhelm attack). Negative impacts of such attacks can be reduced by limiting the frequency of sensor readings and by implementing of an effective data aggregation mechanism.

4. Intrusion Detection in Wireless Sensor Networks

Damage caused by unauthorized intrusions into computer systems and networks can be enormous with immense consequences. Consequently, intrusion detection and prevention systems are currently a very important security mechanism used in modern networks [29–31]. The spread of wireless networks has posed some new challenges and demands for IDS (intrusion detection system) development [32, 33]. Appearance and spread of WSNs requested development of IDS adjusted especially for the WSN. Development and implementation of intrusion detection systems designed for WSNs are still an intensive research area [34–38]. Due to constrained resources and other influencing factors, the implementation of IDS into a WSN represents a great challenge. Some of the important factors that affect the intrusion detection problem in WSNs are network topology, node mobility (mobile or stationary nodes), openness (allowed access for new nodes), current application, environment, routing algorithm, use of encryption, and interconnection with other networks.

Although there are some recent proposals of the intrusion detection systems for WSNs, generally they are intended for the conventional WSNs [39, 40]. There are also some attempts to improve routing mechanism in order to mitigate some types of attacks [41]. Therefore, there is still a lack of adequate IDS especially adapted for IPv6-based WSN with full IPv6 support implemented. The proposed IDS aspires to contribute to solution for this problem. In respect of detection methods and algorithms, the proposed system has certain similarities with some other intrusion detection systems proposed for conventional WSNs. It can be classified as a fully distributed and cooperative system that does not rely on any centralized network infrastructure. Consequently, it is most suitable for flat network infrastructures where each node cooperatively participates in all decisions and actions. There are some examples of the recently proposed distributed

systems for conventional WSNs [42, 43]. On the other hand, some recent proposals of the intrusion detection systems for conventional WSNs rely on a hierarchical (multilayer) or clustered network structure [44]. The proposed system implements specification based intrusion detection technique, as probably the best compromise with low false alarm rate and low energy and resource demands. There are some recently proposed IDS for conventional WSNs that also implement specification based detection [45], while some examples rely on the misuse based or anomaly based detection [46]. Some proposed solutions deal with mobility of network nodes [47]. Some authors introduce different possible detection methods (based on data mining, machine learning, game theory, or genetic algorithms) which require adaptation for implementation into the IPv6-based WSN [48, 49]. Most of the proposed solutions still focus on certain attack type and reside at particular network layer (usually the application layer) [50–52]. Certainly, in the future the research focus should be on cross-layer solutions integrated into the unique security framework with other security mechanisms.

An intrusion detection system developed for a wireless sensor network should satisfy the following requirements and characteristics: distributed architecture (both for data collection and for decision-making), minimal resource consumption (reducing communication as much as possible), finding a compromise between IDS effectiveness and monitoring area size, local data collection and analysis (without relying on central infrastructure), the fact that node compromise must not disrupt proper network function, the fact that neither node may be considered as absolutely secure and reliable, and the fact that the system should operate in real-time. The proposed distributed system for malicious node detection in the IPv6-based WSN tends to satisfy these requirements as much as possible.

Generally, there are two dominant types of WSN architecture: flat architecture (all sensor nodes are similar and use hop-by-hop communication) and hierarchical architecture (nodes are grouped into clusters, where a cluster head is responsible for routing operations). Network architecture has direct influence on positioning of IDS modules. There are a few typical positioning strategies of IDS modules: promiscuous monitoring (IDS module on every sensor node listening to all traffic inside the range of its receiver), IDS module on every node analysing only packets that it forwards, IDS module on the base station (full centralization), IDS modules on base station's neighbours, and IDS modules on cluster heads. There are some proposed solutions for intrusion detection in conventional WSNs, but most of them are focused on a single specific attack type and do not provide integral network security. Also, they mostly do not support the IPv6, so their implementation into the IPv6-based WSN would require proper adaptations and modifications. There is still a problem remaining and it refers to a lack of a quality and efficient intrusion detection system intended for IPv6-based wireless sensor networks and adapted for all specificities of such environment.

The implementation of several different independent security mechanisms into WSNs makes their maintenance more difficult. Therefore, they have to be integrated through

the unique cross-layer security framework [53]. The unique security framework should integrate different security mechanisms to provide basic security premises, that is, confidentiality, authentication, integrity, and availability. It should provide the possibility of data encryption (implying also the implementation of a secure key management mechanism), ensure secure data routing (supporting multiple and alternative routes), and include techniques for secure node localization and secure data aggregation [54–56]. One of the most important components of the quality security framework should be a system for detection of intrusions and malicious node behaviour.

The proposed distributed adaptive system for detection of intrusions and malicious node behaviour was implemented into the unique security framework for the IPv6-based WSN as its intrusion detection module (along with a cryptographic module, a secure routing module, and a secure data aggregation module).

5. Distributed Adaptive IDS for IPv6-Based WSN

Numerous security issues present in wireless sensor networks directly affect the design of security mechanisms, including the intrusion detection system. Some typical problems are as follows: resource limitation (which causes the need for reduced communication and disables the possibility of using the IPsec and public key cryptography), various possible security threats and attack types (denial-of-service, routing attacks, sinkhole, Sybil, wormhole, etc.), and key management problems.

The intrusion detection system for the IPv6-based WSN has to fulfil some general demands just like in the conventional WSN. It should provide an automated mechanism for attack source identification (a malicious network node), generate proper alert for the rest of the network, and take proper preventive measures. Every action targeted against data, communication, or computing resources can be considered as an attack. In order to properly detect an attack, IDS must be able to distinguish legitimate network activities from abnormal (malicious) ones. It could be a serious problem, since in larger networks possible legitimate activities can be vague and unpredictable. For distinguishing and classification of these activities we usually use one of the three following approaches: misuse detection, anomaly detection, and specification based detection.

The misuse detection technique compares current network activities with known attack signatures (behaviour patterns of known malicious activities). Therefore, it is often called signature-based detection. Its main disadvantage is possible detection of only previously known malicious activities for which the sensor node has a stored signature. The anomaly detection approach includes a learning phase, when the IDS learns the pattern of normal network behaviour. All statistical deviations from normal behaviour may in that case be categorized as malicious behaviour. The main disadvantage of this method is a relatively large number of false alarms. Specification based detection combines properties of these two methods, and it is chosen as the most appropriate

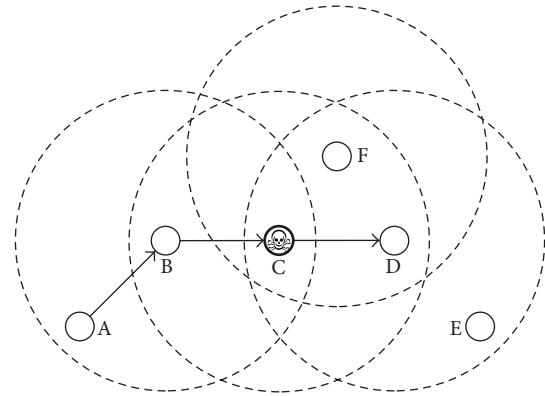


FIGURE 1: Watchdog technique: a possible error example.

method for the proposed IDS for the IPv6-based WSN. Like the anomaly detection technique, it also detects deviations from normal behaviour, but it has manually predefined specifications that describe normal network behaviour. Such approach is less resource demanding, and at the same time it also enables detection of novel attack types.

The proposed IDS is fully distributed and it relies on the cooperative decision-making procedure. Identical IDS modules are implemented on every wireless sensor node, executing cooperative algorithms and communicating with other modules. Since the system is fully distributed, every network node monitors network traffic. The watchdog technique is used for traffic monitoring purposes. It is assumed that every network node has several neighbouring nodes inside the range of its transceiver. Accordingly, all IDS modules listen to their neighbour's traffic and collect data that represent input parameters into collective decision-making process.

Figure 1 illustrates the situation when node A sends a packet to node D (route A-B-C-D). Node C is malicious, and it selectively drops packets addressed to node D. After sending the packet to node C, node B listens to whether node C forwards packet to node D (node B acts as a watchdog). If at the same time node A transmits to node B, due to collision, node B will not be able to determine if node C forwards packets or not. Also, it is possible that node C wrongly concludes that node C successfully forwarded the packet to node D. It will happen if node D or node E starts transmission at the same time. Therefore, it is clear that only one watchdog node is insufficient for successful detection of malicious behaviour. That is why IDS modules collect data from more surrounding watchdog nodes, where nodes cooperatively make final decisions.

At first sight, it seems that traffic monitoring by watchdog nodes will significantly increase power consumption. Fortunately, it is not true, since in most radio communication systems implemented in WSNs sensor nodes already receive packets broadcasted from their neighbours. Therefore, additional power is used only for additional data processing and for communication between IDS modules.

The intrusion detection problem (IDP) includes detection that a certain network node is attacked (compromised) as well

as identification of the attack source. Therefore, a solution (algorithm) to the IDP must satisfy the following properties:

- (i) If a legitimate node indicates possible malicious behaviour of another node, it will join the group of alerted nodes, and a potentially malicious node will be characterized as the attack source.
- (ii) If a malicious activity occurs, after a finite time interval all legitimate nodes from the group of alerted nodes will indicate possible malicious behaviour of the observed node.

The basic idea of cooperative intrusion detection is a mutual exchange of IDS agents (modules) output data. Modules exchange data about suspicious nodes, narrowing the group of possible malicious nodes. It is also possible that a malicious node falsely accuses its neighbours of malicious activities. There are two main conditions for solving the intrusion detection problem: intrusion detection condition (IDC) and neighbourhood conditions (NC). Intrusion detection condition is satisfied if neither network node has an identical alerted set as the malicious node. There are two neighbourhood conditions: all neighbours of the malicious node are alerted (first condition) and if two or more nodes are suspected by a majority of nodes, then all legitimate suspected nodes must have nonalerted neighbours (second condition). The intrusion detection problem (IDP) can be solved by a deterministic algorithm if (and only if) intrusion detection condition (IDC) or neighbourhood conditions (NC) are satisfied.

The Contiki operating system was used as a software platform for the implementation of a distributed adaptive intrusion detection system [57]. Contiki was one of the first operating systems for sensor networks that supports the IP. First, it was IPv4 support, and then after 6LoWPAN specification the IPv6 support was added. The implementation of IPv6 support was followed by support for the RPL. Support for IPv6 and RPL were the reasons for using the Contiki operating system. For testing and simulation purposes, we used the COOJA simulator, since it fully supports the Contiki OS at multiple levels, from machine code level to operating system level [58].

The system for malicious node detection in the IPv6-based WSN is a fully distributed system, based on collaborative algorithms without relying on central infrastructure. IDS modules (agents) are implemented on every node in the WSN. The main task of the IDS agent is to monitor neighbouring nodes (within transceiver range) and to participate in the collective decision process. The implemented algorithm operates independently of the primary sensor network application. The system is fully adapted for the protocol stack in the IPv6-based WSN (Figure 2).

The IDS agent core operates on the application layer. The UDP is used as the transport layer protocol, while the RPL is implemented as a routing protocol [59]. The 6LoWPAN adaptation layer is implemented for IPv6 header compression purposes, enabling the efficient transfer of IPv6 packets over the IEEE 802.15.4 physical layer [60]. Functionality of the IDS agent can be divided into the following three

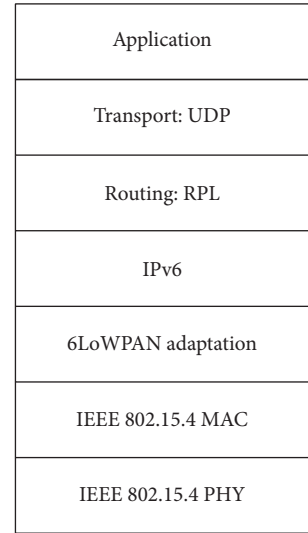


FIGURE 2: IPv6-based WSN protocol stack.

basic components: network monitoring (data gathering by monitoring neighbours' network traffic), decision-making (a collective process based on exchanged data through mutual communication and collaboration between IDS agents), and reaction (action in case malicious behaviour of a certain node has been detected). After sending the packet, every node monitors its neighbours in order to determine whether they forward packets further toward their final destination or not (a watchdog approach). Nonforwarded packets may indicate malicious behaviour, since in the WSN surroundings many other factors may also influence packet delivery success (e.g., collisions or node failures).

Therefore, the intrusion detection system defines a finite time interval in which the IDS module counts dropped packets on neighbouring nodes. The duration of this interval is a variable and adjustable parameter. Also, the threshold is defined that represents the maximal number of allowed packet drops. If dropped packets outnumber the threshold, the observed node is considered suspicious. This threshold is also a variable and configurable parameter that can be defined according to current application and network conditions. Due to a large variety of WSNs (regarding number and density of nodes, link capacity, and data amount) and their possible applications, it is impossible to set universal values of these parameters (monitoring interval and threshold) for all situations. Parameter values should be adjusted for every particular application. The proposed IDS uses a specification based detection approach, since other approaches (misuse detection or anomaly detection) would be more resource demanding. The structure of the IDS for the IPv6-based WSN is presented in Figure 3.

An intrusion detection agent consists of two main modules: a local detection module and a cooperative detection module. These modules are interconnected and together they participate in the process of detecting malicious sensor nodes. These two modules are also connected with a module for local traffic monitoring and with communication modules (for communication with other IDS agents and with the

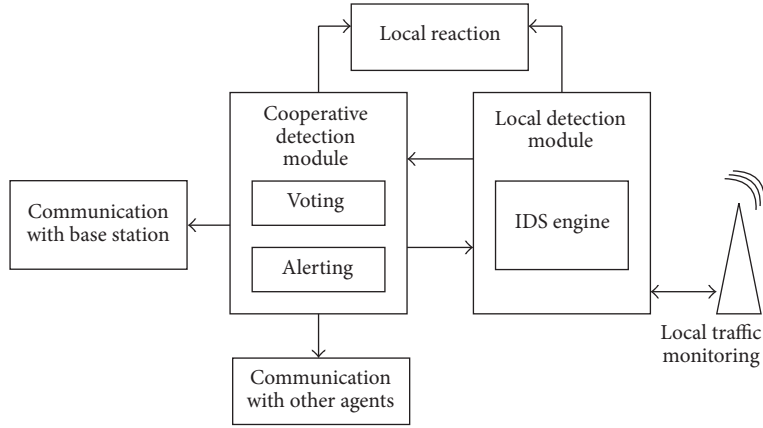


FIGURE 3: Intrusion detection system structure.

base station). Communication modules are indispensable for construction of the distributed system, since its proper functioning is based on cooperation of many IDS agents.

5.1. Local Detection Module. A local detection module is connected to a local traffic monitoring module that gathers data required for local decisions. This module analyses gathered data and creates a list of suspected neighbouring nodes (according to previously defined specifications). The local detection module alerts other neighbouring nodes about its suspect list. Every node creates a list of its suspected neighbours (neighbours whose behaviour can be characterized as possibly malicious). Also, the local detection module estimates the probability of malicious behaviour of its neighbours. This probability estimation is based on the number of forwarded and dropped packets during the observed time interval. Every node s estimates the probability of malicious behaviour of its neighbour i according to

$$p_m(i) = 1 - \frac{n_f(i)}{n_r(i)}, \quad \forall i \in N(s). \quad (1)$$

$p_m(i)$ is the estimated probability that neighbouring node i behaves maliciously, $n_r(i)$ is the number of packets that node i receives, $n_f(i)$ is the number of packets that node i forwards, and $N(s)$ is a set of neighbouring nodes of node s . If estimated probability $p_m(i)$ exceeds the predefined threshold value, node i will be added to the suspect set $D(s)$ of node s . Node s exchanges its list of suspected nodes (together with estimated probabilities) with other network nodes. After alert messages (which contain lists of suspected nodes and estimated malevolence probabilities) are exchanged, when all nodes gather messages from other nodes, the cooperative detection module is being activated. The cooperative detection module will make the final decision about suspected nodes. A trivial case is the situation when a certain sensor node has only one neighbouring node on its suspect list with the estimated malevolence probability equal to 1. In that case, the local detection module can directly activate local reaction and communication modules, without any need for

the cooperative decision procedure. Figure 4 represents the operating algorithm of the local detection module.

5.2. Cooperative Detection Module. The main task of the cooperative detection module is to make the final decision about behaviour character of suspected sensor nodes. The module makes this decision cooperatively with other nodes. The decision is made after executing the cooperative algorithm that implements a majority voting mechanism about node malevolence. Input data for the cooperative decision-making process are suspect node lists together with estimated malevolence probabilities. The final malevolence probability for every network node is calculated after execution of cooperative algorithms. If this value outnumbers the predefined threshold, the corresponding node will be finally declared as malicious. The final probability for every node is calculated by (2), where $p_M(s_i)$ is the final calculated malevolence probability for node s_i . Consider

$$p_M(s_i) = \frac{1}{n} \sum_{i=1}^n p_m(i), \quad \forall s_i \in S. \quad (2)$$

This probability is calculated as the average of all estimated probabilities $p_m(i)$ by all nodes that put node s_i into the suspected set. If probability $p_M(s_i)$ is above the predefined threshold value, the corresponding node will be considered malicious. In case more probabilities are above the threshold, the node with most votes will be classified as malicious. Node with the largest estimated malevolence probability $p_M(s_i)$ will be declared malicious if some nodes have an equal number of votes. In case behaviour of certain nodes is marked as malicious, the cooperative detection module activates communication modules in order to inform the base station and other network nodes. Malicious nodes will be excluded from the network by local reaction modules. Figure 5 presents the algorithm for the cooperative detection module.

5.3. Testing Scenarios. Behaviour of the proposed system for malicious node detection in the IPv6-based WSN was analysed and tested through different scenarios typical of sensor

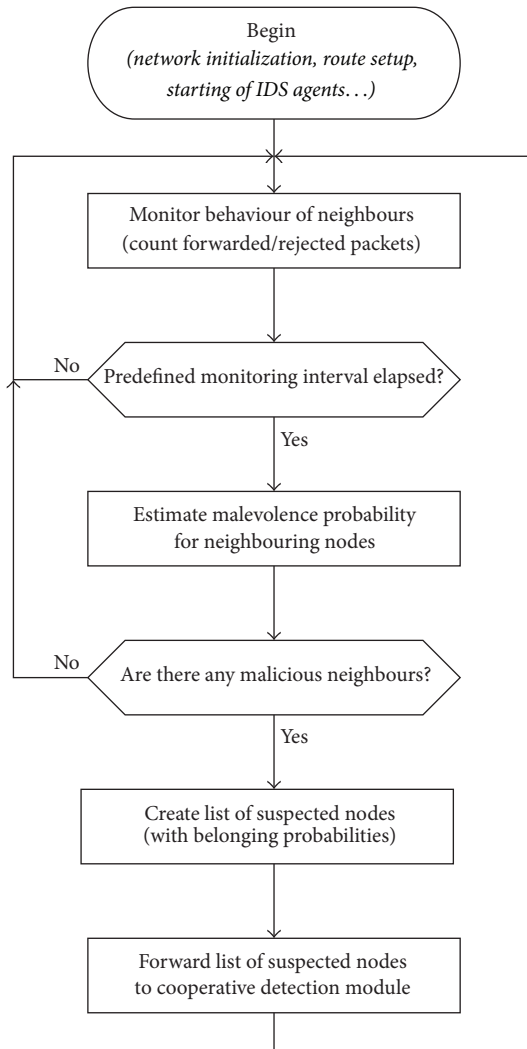


FIGURE 4: Local detection module algorithm.

networks. The possibility of successful detection of nodes' malicious behaviour and the system influence on normal network functioning (primarily on power consumption and bandwidth occupation) were the focus of analyses and tests.

All tests were performed in three different networks. The first network consists of 6 nodes (5 sensor nodes and the base station), the second network consists of 10 nodes (9 sensor nodes and the base station), and the third network consists of 17 nodes (16 sensor nodes and the base station). These topologies were chosen because they reflect a large variety of practical sensor network applications. In all testing scenarios, the base station is located near the edge of the network area in order to enforce multihop communication. All network nodes have the same physical characteristics (a homogenous network) and the implemented IPv6 stack.

Three scenarios were analysed in every network (6, 10, and 17 nodes). The difference between these scenarios lies in the probability of successful sending and receiving of data packets. The first scenario represents a reference ideal case, where this probability equals 100%. However, the

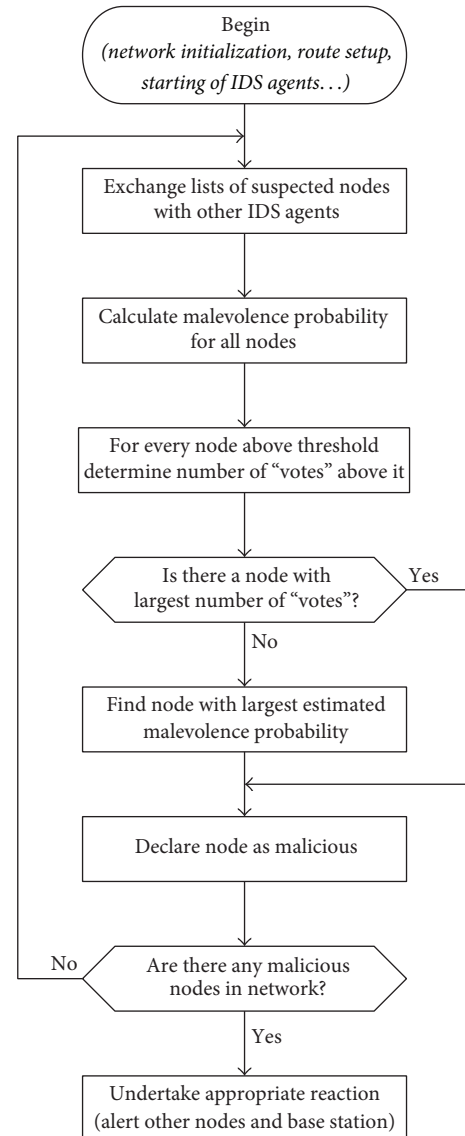


FIGURE 5: Cooperative detection module algorithm.

packet loss in WSN is common due to interference, node failures, or collisions and sometimes malicious activities. It is very important to consider these situations, since packet losses and a need for retransmission directly affect network performance and resource consumption and also complicate (in extreme situations even prevent) detection of malicious activities. For that reason, beside ideal scenario two additional scenarios in all three networks are analysed. In the second scenario, in all networks Rx/Tx success ratio was 80%, and in the third scenario it was 60%.

Previous analysis of the WSN without intrusion detection system was performed for performance testing purposes (total of 9 scenarios, three scenarios in three different networks), in order to analyse normal network behaviour without any IDS influence on WSN performance. Thereby, sensor nodes collect data from their surroundings (temperature, humidity, and illumination) and send them to the base

station periodically (every minute). In all performed tests, the network was monitored during the one-hour interval. In every testing scenario, after network initialization and route establishment, the number of neighbours and the number of hops to the base station were recorded for every node. Since in observed scenarios all nodes were static, these values are generally related to network topology. Therefore, for the same network they did not significantly change depending on the analysed scenario (minor changes may occur if packet loss causes network reconfiguration and changes in some parts of the routes). The following parameters were observed and recorded for all testing scenarios: the number of received packets (for every node), the number of lost packets, ETX metrics (which shows the required number of retransmissions on individual links), an average radio duty cycle (for every network node), and power consumption (average for every network node). Total power consumption for every node includes the following four components: CPU consumption, consumption in low power mode (LPM), and radio transceiver consumption in listen and in transmit mode. The results obtained are used for comparison with identical scenarios, but with the proposed intrusion detection system implemented into the network (topology and all other parameters remained unchanged) in order to analyse the impact of the IDS on normal network operation. The goal was to investigate if the implemented IDS distorted network performances and whether it causes significant power consumption increment. Therefore, after IDS implementation, the analysis was repeated through all nine characteristic scenarios.

In addition to performance testing, the analysis of malicious behaviour detection capabilities of the proposed IDS was also performed. Detection capability analysis was also accomplished through the nine mentioned scenarios (three characteristic scenarios in three different networks), since detection capability is directly influenced by the total number of nodes and the number of networking nodes, as well as the number of unintentionally dropped packets. Every analysed scenario included one malicious node that selectively forwards packet, where it drops 80% of the packets. Two different situations were taken into consideration for every analysed scenario. In the first case, a malicious node selectively drops packets without accusing its neighbours of malicious behaviour. In the second case, a malicious node falsely accuses its neighbours of malicious behaviour, trying to disrupt IDS detection capabilities. IDS detection capabilities were analysed through all described scenarios, where the system also estimates malevolence probabilities of network nodes. The performed analyses resulted in certain conclusions about the influence of the number of nodes, the number of dropped packets, and malicious node behaviour on detection capabilities of the proposed IDS.

6. Result Analysis

6.1. IDS Performance Analysis. Performance analysis of the proposed IDS was performed through 9 different scenarios in three previously described different networks (6 nodes, 10 nodes, and 17 nodes). The first testing network includes

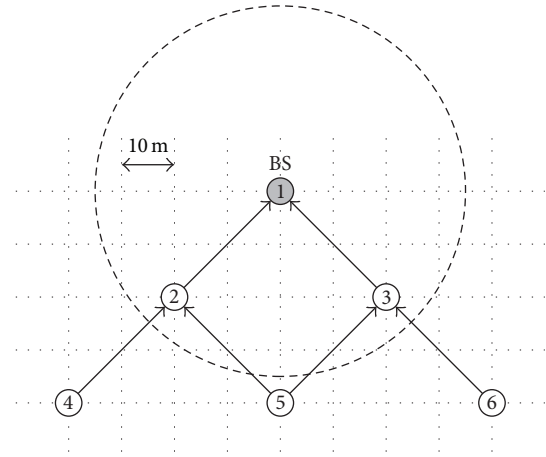


FIGURE 6: Six-node network topology.

6 nodes (5 sensor nodes and the base station), as shown in Figure 6.

Node 1 is the base station, while the others (2–6) are regular sensor nodes. Raster pattern size in the figure matches 10 m distance. A radio transceiver range is set to 30 meters (circular area), while the interference area radius equals 50 meters. These values directly influence network topology and the establishment of the routes to the base station, since the possibility of direct communication between nodes depends on their transceiver range. In a 6-node network, the base station is within the range of nodes 2 and 3. Neighbouring nodes are nodes that can directly communicate with each other. Therefore, a neighbouring node of node 4 is node 2, while a neighbouring node of node 6 is node 3. Neighbouring nodes of node 5 are nodes 2 and 3. Accordingly, nodes 2 and 3 have three neighbours, and node 5 has two neighbours, while nodes 4 and 6 have one neighbouring node. Consequently, routes from nodes 4, 5, and 6 to the base station include 2 hops, while nodes 2 and 3 can directly communicate with the base station.

After network initialization, every network node periodically (once a minute) sends its sensor readings to the base station (temperature, humidity, and illumination). Three scenarios with a different Rx/Tx success ratio were analysed. This ratio is 100%, 80%, and 60%, in the first, second, and third scenario, respectively. All tests were performed with and without the intrusion detection system implemented, in order to draw a conclusion about the IDS impact on network performance. Values of observed parameters (described in Section 5.3) are collected for all sensor nodes, and their summarized average values for 6-network nodes are given in Table 1.

In the first analysed scenario (which represents an ideal case, with no packet loss), the increased number of received packets can be noticed after the implementation of the IDS. It was expected since additional traffic is generated by the IDS agents. However, it is important to notice that there is no significant change in total energy consumption (since energy is the most limited resource in the WSN) after the IDS implementation. Some minimal deviations in recorded

TABLE 1: Performance analysis of 6-node network.

6 nodes	Received packets	Lost packets	Hops to BS	ETX	Energy consumption (mW)				Duty cycle (%)		
					CPU	LPM	Listen	Transmit	Total	Listen	Transmit
Scenario 1 (Rx/Tx = 100%)											
w/o IDS	59.200	0.000	1.600	1.008	0.065	0.162	0.391	0.033	0.650	0.651	0.062
w/ IDS	65.800	0.000	1.600	1.002	0.064	0.162	0.389	0.029	0.649	0.649	0.054
Scenario 2 (Rx/Tx = 80%)											
w/o IDS	58.400	0.600	1.600	2.256	0.083	0.161	0.419	0.146	0.808	0.699	0.274
w/ IDS	65.800	0.600	1.600	2.057	0.083	0.161	0.423	0.138	0.806	0.706	0.260
Scenario 3 (Rx/Tx = 60%)											
w/o IDS	50.600	7.000	1.629	5.991	0.135	0.159	0.514	0.484	1.292	0.857	0.912
w/ IDS	57.800	8.800	1.600	5.793	0.134	0.159	0.521	0.498	1.312	0.868	0.938

values can be explained by the application of stochastic algorithms and inability to measure real consumption very precisely. In the second scenario (with the Rx/Tx success ratio of 80%), smaller packet loss can be noticed in spite of acknowledgement and retransmission mechanisms used. An increment of the ETX compared to the first scenario shows that retransmission of some packets was necessary. A need for packet retransmission leads to an increased transceiver activity, which can be observed from their duty cycle. Since the radio transceiver is the most energy demanding part of the sensor node, its increased activity leads to an increase in energy consumption compared to the first scenario. However, the implementation of the IDS still does not bring any significant difference in energy consumption (compared to the same scenario without the IDS). The third scenario additionally increases the need for packet retransmission (the indicator is increased ETX), since the packet Rx/Tx success ratio is reduced to 60%, resulting in increased energy consumption. In spite of the retransmission mechanism, an increased number of lost packets were recorded. In the third scenario with the implemented IDS, a slight increase in energy consumption compared to the case without the IDS can be noticed.

The second testing network consists of 10 nodes (9 sensor nodes and the base station). The topology of second testing network is shown in Figure 7.

As in the first network (6 nodes), testing was performed through three scenarios, where the Rx/Tx success ratio was 100%, 80%, and 60%, respectively. In a 10-node network, nodes have from 2 to 5 neighbouring nodes (nodes 3, 7, and 9 have 2 neighbours; nodes 1, 6, and 8 have 3 neighbours; nodes 2 and 4 have 4 neighbours; and node 5 has 5 neighbours). Nodes 1, 2, 4, and 5 have one hop to the base station, nodes 3, 6, 7, and 8 have two hops, and node 9 has three hops. Average values of observed parameters in a 10-node network are summarized in Table 2.

The first analysed scenario in a 10-node network also represents the ideal case, without lost packets and any need for retransmission. The implementation of the IDS introduces a small amount of additional network traffic (generated by the IDS agents), without a significant influence on total energy consumption. Total average energy consumption of the first scenario in a 10-node network is comparable to an equivalent

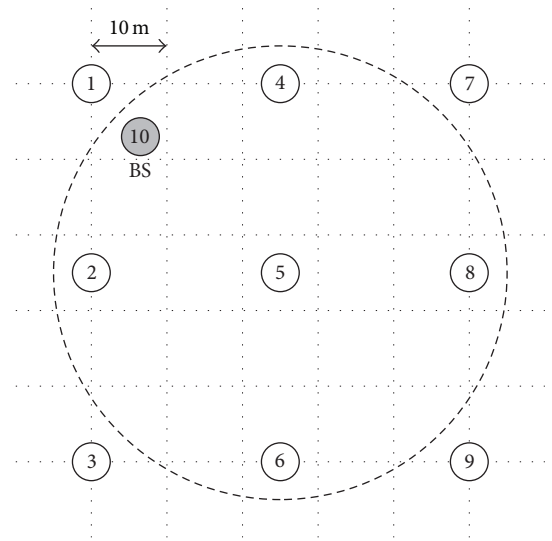


FIGURE 7: 10-node network topology.

scenario in a 6-node network. A decreased probability of successful packet transmissions in the second scenario causes packet loss and retransmissions. An increased transceiver activity increases energy consumption, which is comparable with consumption in an equivalent scenario in a 6-node network. The implementation of the IDS slightly increases energy consumption, but not to the extent of making the IDS implementation not justified. Further decrement of the Rx/Tx success ratio in the third scenario (to 60%) additionally increases the number of required retransmissions (the indicator is the ETX metrics) and energy consumption. Total consumption rises after the implementation of the IDS, but the increment is less than 10% and does not jeopardize validity of the IDS implementation.

Three different scenarios (with the Rx/Tx success ratio of 100%, 80%, and 60%) were also analysed in a 17-node network. The topology of the third testing network is shown in Figure 8 (nodes 1–16 are regular sensor nodes, and node 17 is the base station).

In a 17-node network, sensor nodes have 2 to 5 neighbours (nodes that are in a direct transceiver range). The minimal

TABLE 2: Performance analysis of 10-node network.

10 nodes	Received packets	Lost packets	Hops to BS	ETX	Energy consumption (mW)				Duty cycle (%)		
					CPU	LPM	Listen	Transmit	Total	Listen	Transmit
Scenario 1 (Rx/Tx = 100%)											
w/o IDS	62.222	0.000	1.667	1.000	0.064	0.162	0.392	0.029	0.647	0.654	0.055
w/ IDS	67.444	0.000	1.667	1.000	0.065	0.162	0.394	0.032	0.652	0.657	0.060
Scenario 2 (Rx/Tx = 80%)											
w/o IDS	58.667	1.222	1.690	1.766	0.081	0.161	0.431	0.133	0.806	0.718	0.250
w/ IDS	65.889	0.667	2.079	1.914	0.098	0.161	0.473	0.219	0.951	0.789	0.412
Scenario 3 (Rx/Tx = 60%)											
w/o IDS	51.889	7.333	1.692	5.148	0.122	0.160	0.527	0.409	1.218	0.878	0.770
w/ IDS	50.556	10.556	1.718	4.554	0.134	0.159	0.544	0.478	1.315	0.907	0.899

TABLE 3: Performance analysis of 17-node network.

17 nodes	Received packets	Lost packets	Hops to BS	ETX	Energy consumption (mW)				Duty cycle (%)		
					CPU	LPM	Listen	Transmit	Total	Listen	Transmit
Scenario 1 (Rx/Tx = 100%)											
w/o IDS	59.500	0.000	2.563	1.001	0.068	0.161	0.405	0.042	0.676	0.675	0.079
w/ IDS	66.625	0.000	2.563	1.000	0.069	0.161	0.407	0.043	0.680	0.678	0.081
Scenario 2 (Rx/Tx = 80%)											
w/o IDS	58.375	1.250	2.582	2.001	0.108	0.160	0.502	0.276	1.047	0.837	0.520
w/ IDS	64.563	1.750	2.648	2.029	0.110	0.508	0.847	0.289	1.068	0.847	0.545
Scenario 3 (Rx/Tx = 60%)											
w/o IDS	44.267	13.867	2.366	5.574	0.160	0.159	0.644	0.605	1.568	1.073	1.140
w/ IDS	44.125	13.313	2.538	5.714	0.168	0.158	0.657	0.666	1.649	1.095	1.255

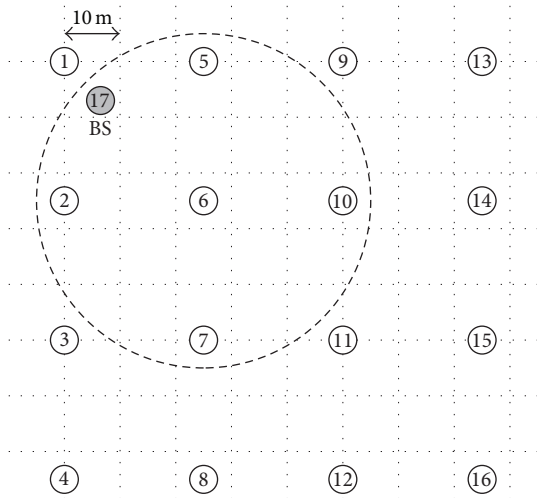


FIGURE 8: 17-node network topology.

distance from the base station is one hop (for nodes 1, 2, 5, and 6), while maximal distance is 5 hops (for node 16). Average values of observed parameters in a 17-node network are summarized in Table 3.

Similarly to 6-node and 10-node networks, the first scenario in a 17-node network is the ideal case without packet losses and retransmissions. Also, there is no significant

difference in power consumption for this scenario before and after the IDS implementation. In the second scenario, some packet losses appear, and packet retransmissions increase average energy consumption. Average energy consumption is slightly larger than in equivalent scenarios in 6-node and 10-node networks, but the implementation of the IDS in this scenario does not increase energy consumption significantly either. The third scenario in a 17-node network (the Rx/Tx success ratio is 60%) records the largest number of lost packets and retransmissions and consequently the smallest number of received packets. Moreover, in one case, due to excessive packet loss, the furthest node (node 16, i.e., 5 hops far from the base station) could not communicate with the base station. As expected, the third scenario in a 17-node network records the highest energy consumption. However, even in this scenario the implementation of the IDS does not significantly increase energy consumption.

The performed analyses show that the implementation of the proposed system for detection of malicious node behaviour in the IPv6-based WSN does not significantly degrade network performance. Also, it is a very important fact that the implementation of the proposed IDS does not lead to a significant increase in energy consumption as the most limited resource in the WSN. Moreover, in some analysed scenarios the difference in power consumption with and without the IDS is almost indistinguishable (because its magnitude is smaller than possible errors that can be

expected in the measurement process), while in other cases the difference does not exceed several percent.

Energy efficiency (e.g., very small additional energy demands) represents one of the two most important preconditions that the IDS must satisfy in order to consider its practical application and implementation into the WSN. Another important prerequisite is its capability for successful detection of malicious network nodes. Therefore, the following section analyses malicious node detection possibilities of the proposed IDS.

6.2. IDS Detection Capabilities Analysis. The analysis of malicious node behaviour detection capabilities for the proposed IDS was performed (similarly to its performance analysis) in three previously described networks with 6, 10, and 17 network nodes, respectively. In every network, detection capability was tested in all three characteristic scenarios (as in the case of performance testing) with the Rx/Tx success ratio of 100%, 80%, and 60%. It is important to test the IDS in such environment, where a malicious activity is not the only possible cause of packet dropping, but the packets can be lost during normal network operation (e.g., due to noise and collisions). A noisy and lossy environment makes malicious node detection more complicated.

In every analysed scenario, one malicious node was intentionally installed into the WSN. The malicious node selectively forwards packets such that it drops 80% of packets, while it forwards 20% of packets toward their destination. Two different cases were considered in every analysed scenario. In the first case, a malicious node just selectively forwards traffic in a described way (80% drops, 20% forwards). In the second case, besides selective forwarding, a malicious node falsely accuses its neighbouring nodes of the same malicious behaviour, and in this way it intentionally aggravates correct detection of the IDS.

A feature of the proposed IDS is its capability to estimate the malevolence probability besides characterization of a sensor node as malicious or legitimate. For testing purposes, the probability threshold is 50% (a node is considered malicious if the malevolence probability is greater than 50%). This threshold is adjustable and can be adapted to specific application requirements. In given tables, every row includes malevolence probabilities that every node estimates for its neighbouring nodes. The last row includes calculated final malevolence probabilities for every node. Some cells are empty since corresponding nodes are not neighbours, and therefore there is no estimated probability. The goal of the analysis is to determine the influence of different factors (e.g., the number of nodes, lost packets, and behaviour of the malicious node) on successful detection of a malicious node.

In a 6-node network (Figure 6), a malicious node is node 3. Table 4 contains estimated malevolence probabilities (in percent) for the first scenario (the Rx/Tx success ratio is 100%) in a 6-node network. The first number in each cell represents the estimated malevolence probability when a malicious node does not try to falsely accuse its neighbours (scenario 1a). The second number in each cell (printed in italics) represents the estimated malevolence probability when a malicious node additionally falsely accuses its neighbours

TABLE 4: Detection in 6-node network, scenario 1.

	2	<u>3</u>	4	5	6
2			0.0/0.0	0.0/0.0	
<u>3</u>				0.0/ <u>80.3</u>	0.0/ <u>80.3</u>
4	0.0/0.0				
5	0.0/0.0	80.3/80.3			
6		80.3/80.3			
p_M (%)	0.0/0.0	<u>80.3/80.3</u>	0.0/0.0	0.0/80.3	0.0/80.3

TABLE 5: Detection in 6-node network, scenario 2.

	2	<u>3</u>	4	5	6
2			0.0/0.0	1.5/1.5	
<u>3</u>				1.5/ <u>82.1</u>	3.0/ <u>83.3</u>
4	0.0/0.0				
5	0.0/0.0	79.1/79.1			
6		77.9/77.9			
p_M (%)	0.0/0.0	<u>78.5/78.5</u>	0.0/0.0	1.5/41.8	3.0/83.3

(scenario 1b). For example, the value “0.0/80.3” in the third row, the sixth column, means that in scenario 1a node 3 estimates the malevolence probability of 0.0% for node 6, and in scenario 1b node 3 estimates the malevolence probability of 80.3% for node 6 (it falsely accuses its neighbour).

In scenario 1a, the IDS easily draws a correct conclusion that node 3 is a malicious node (with estimated malevolence probability $p_M = 80.3\%$). In scenario 1b (where node 3 falsely accuses its neighbours), there are three nodes (nodes 3, 5, and 6) for which estimated malevolence probability p_M exceeds the threshold value of 50% ($p_M = 80.3\%$). Nevertheless, the IDS still makes a correct decision and designates node 3 as malicious since there are two estimates for node 3 that are above the threshold (by nodes 5 and 6), while nodes 5 and 6 have only one estimation above the threshold. However, it is obvious that false accusations (by malicious nodes) may significantly complicate the detection procedure and even cause incorrect conclusions.

Table 5 shows estimated malevolence probabilities for the second scenario in a 6-node network, where the Rx/Tx success ratio is 80%.

It is obvious that in scenario 2a detection of a malicious node was successful (the malevolence probability for node 3 equals 78.5%). But it is also apparent that additional packet losses present in this scenario cause the probability p_M to be somewhat lower than in the first scenario (which represents an ideal lossless case). For the same reason, some estimated malevolence probabilities for other nodes also appear. In scenario 2b (where node 3 falsely accuses its neighbours), there are two estimations above the threshold (for node 3 and node 6). A correct IDS decision was made since for node 3 there are two estimations above the threshold (while for node 6 there is only one).

Table 6 contains estimated malevolence probabilities for the third scenario in a 6-node network, where the Rx/Tx success ratio is 60%.

TABLE 6: Detection in 6-node network, scenario 3.

	2	3	4	5	6
2			22.4/22.4	21.5/21.5	
3				21.5/ <u>85.1</u>	22.4/ <u>85.1</u>
4	0.0/0.0				
5	0.0/0.0	63.2/63.2			
6		62.6/62.6			
p_M (%)	0.0/0.0	<u>62.9/62.9</u>	22.4/22.4	21.5/ <u>53.3</u>	22.4/ <u>85.1</u>

In scenario 3a, the IDS makes a correct decision and declares node 3 as malicious. However, it is noticeable that increased packet loss (Rx/Tx is lowered to 60%) reduces estimation quality (the malevolence probability is 62.9%), while at the same time malevolence probabilities for legitimate nodes increase but are still below the threshold. In scenario 3b, where a malicious node falsely accuses its neighbours, malevolence probabilities for three nodes (nodes 3, 5, and 6) exceed the threshold. The IDS also makes a correct decision in this case since for node 3 (a malicious node) there are two estimations above the threshold, while nodes 5 and 6 have one estimation above the threshold.

In a 10-node network (Figure 7), node 8 was deliberately made malicious for IDS detection testing purposes. Testing was performed for all three characteristic scenarios (similarly to a 6-node network). Table 7 represents results for the first scenario (Rx/Tx = 100%).

In the first case (scenario 1a), the IDS correctly recognizes node 8 as a malicious node with malevolence probability rating of 80.1%. In scenario 1b (where node 8 falsely accuses its neighbours), the IDS also draws a correct conclusion. It is noticeable that in scenario 1b some estimated malevolence probabilities emerged for other nodes (due to false accusations by node 8), but all are below the threshold value.

Table 8 presents testing results of the second scenario in a 10-node network (Rx/Tx = 80%).

Obviously, the IDS will correctly recognize a malicious activity of node 8, although in this scenario some malevolence estimations for other (legitimate) nodes occurred (due to certain packet loss). However, these probabilities by value are significantly below the threshold of 50%. Actually, these probabilities are even lower than estimated probabilities in the corresponding scenario of a 6-node network. This is because in the network with a larger number of nodes every node (on average) has more neighbours, making final estimations more accurate. Malicious node detection was also successful in scenario 2b, where a malicious node falsely accuses its neighbours. However, it is obvious that false accusations increase the probability of wrong malevolence estimations for legitimate nodes (which still remain below the threshold).

The results of the third testing scenario (Rx/Tx = 60%) in a 10-node network are presented in Table 9.

In scenario 3a, the IDS successfully detects a malicious node, but the quality of estimation (the value of final malevolence probability p_M) decreases. The final malevolence probability for a malicious node is lower than in previous scenarios

but still above the threshold ($p_M = 60.9\%$). At the same time, p_M values of incorrect estimations increase, so it happened that for node 9 the value of p_M also exceeds the threshold ($p_M = 52.75\%$) although it is the legitimate node. Further, it is visible that false accusation data that a malicious node puts into the network in scenario 3b significantly complicates a correct decision-making process. In this example, node 9 has the largest malevolence probability p_M ($p_M = 70.6\%$), which is actually legitimate node. Probability p_M also exceeds the threshold for node 8 ($p_M = 60.9\%$), which is in fact malicious. In this example, the IDS still drew a correct conclusion since there are two estimations above the threshold for node 8 (by nodes 5 and 7) and one estimation for node 9 (by node 8). Nevertheless, it should be noticed that the estimation for node 9 by node 6 was very close to the threshold (47.1%). Although it was an incorrect estimation (caused by packet losses that occurred), it could possibly happen that this estimation exceeds the threshold. In that case, the IDS would draw an incorrect conclusion that a malicious node is node 9. Furthermore, it is apparent that node 9 (again due to significant packet losses) made an incorrect estimation about node 8 (p_M was only 25.8%), which also aggravates the decision-making process.

In a 17-node network (Figure 8), for testing purposes, the malicious node was node 10. The results of the intrusion detection process for the first scenario (Rx/Tx = 100%) in a 17-node network are presented in Table 10.

In scenario 1a, in a 17-node network (an ideal case, with no packet losses), the IDS easily detects malicious activities of node 10. In scenario 1b, there are some malevolence estimations for legitimate nodes (caused by false accusations by node 10), but they are all below the threshold.

Table 11 shows testing results for the second scenario in a 17-node network (Rx/Tx = 80%).

In scenario 2a, in a 17-node network, malicious node detection was successful, but some malevolence estimations for legitimate nodes occur due to packet losses (all below the threshold). In scenario 2b (where node 10 falsely accuses its neighbours), detection is also successful, but the estimated malevolence probabilities for some legitimate nodes also increased due to false accusations by node 10 (they are still below the threshold).

Table 12 presents results of the third testing scenario in a 17-node network (Rx/Tx = 60%).

The results show that detection was successful in scenario 3a of a 17-node network, but it is obvious that increased packet loss causes the increment of wrong malevolence estimations for legitimate nodes (e.g., nodes 11 and 14 give estimations of 44.0% and 54.8% for the malevolence probability of malicious node 10, while at the same time for legitimate node 15 they give estimated malevolence probabilities of 53.2% and 66.1%). False accusations by node 10 (in scenario 3b) additionally increase incorrect estimations about malevolence of legitimate nodes. Fortunately, these estimations are still below the threshold, owing to correct estimations of a larger number of legitimate nodes that reduce a negative impact of false accusations by a malicious node.

Tests and analyses performed through more different characteristic scenarios showed that the system proposed for

TABLE 7: Detection in 10-node network, scenario 1.

	1	2	3	4	5	6	7	<u>8</u>	9
1		0.0/0.0		0.0/0.0					
2	0.0/0.0		0.0/0.0		0.0/0.0				
3		0.0/0.0				0.0/0.0			
4	0.0/0.0				0.0/0.0		0.0/0.0		
5		0.0/0.0		0.0/0.0		0.0/0.0		80.1/80.1	
6			0.0/0.0		0.0/0.0				0.0/0.0
7				0.0/0.0				80.1/80.1	
<u>8</u>					0.0/ <u>80.6</u>		0.0/ <u>80.6</u>		0.0/ <u>80.1</u>
9						0.0/0.0		80.1/80.1	
p_M (%)	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/20.2	0.0/0.0	0.0/40.1	<u>80.1/80.1</u>	0.0/40.1

TABLE 8: Detection in 10-node network, scenario 2.

	1	2	3	4	5	6	7	<u>8</u>	9
1		0.0/0.0		0.0/0.0					
2	0.0/0.0		1.5/1.5		0.0/0.0				
3		1.5/1.5				1.5/1.5			
4	0.0/0.0				0.0/0.0		0.0/0.0		
5		0.0/0.0		0.0/0.0		0.0/0.0		80.6/80.6	
6			1.5/1.5		0.0/0.0				4.5/4.5
7				0.0/0.0				80.6/80.6	
<u>8</u>					0.0/ <u>83.6</u>		0.0/ <u>83.6</u>		4.5/ <u>81.5</u>
9						4.5/4.5		79.8/79.8	
p_M (%)	0.0/0.0	0.5/0.5	1.5/1.5	0.0/0.0	0.0/20.9	2.0/2.0	0.0/41.8	<u>80.3/80.3</u>	4.5/43.0

TABLE 9: Detection in 10-node network, scenario 3.

	1	2	3	4	5	6	7	<u>8</u>	9
1		4.5/4.5		0.0/0.0					
2	4.5/4.5		23.1/23.1		0.0/0.0				
3		3.4/3.4				23.7/23.7			
4	0.0/0.0				0.0/0.0		9.2/9.2		
5		4.5/4.5		0.0/0.0		31.3/31.3		82.3/82.3	
6			16.6/16.6		0.0/0.0				47.1/47.1
7				0.0/0.0				74.7/74.7	
<u>8</u>					0.0/ <u>82.3</u>		7.8/ <u>89.2</u>		58.4/ <u>94.0</u>
9						9.8/9.8		25.8/25.8	
p_M (%)	2.3/2.3	4.1/4.1	19.9/19.9	0.0/0.0	0.0/20.6	21.6/21.6	8.5/49.2	<u>60.9/60.9</u>	<u>52.75/70.6</u>

malicious node detection in the IPv6-based WSN successfully detects presence of a malicious network node. Thereby, the proposed system satisfies an important prerequisite for the implementation into the IPv6-based WSN (in addition to necessary energy efficiency and a minimal influence on network performance and its proper operation). Unlike most other IDS known in conventional WSNs, the proposed system also gives the estimation of the node malevolence probability (while other systems usually just declare a node as malicious or legitimate). The performed tests showed the influence of different parameters on the decision-making process and the quality of estimation. Packet loss present in the network due to noise, collisions, or failures has a

negative impact on the quality of malevolence probability estimation. It is sometimes difficult to resolve the real reason for packet loss, that is, whether it is one of the aforementioned reasons or a malicious activity of the node that intentionally drops or selectively forwards packets. Furthermore, presence of packet loss may cause legitimate nodes to be considered malicious with some probability, which may, in extreme cases, exceed the threshold value (a situation where a malicious node is not detected or a legitimate node is incorrectly designated as malicious). A real sensor network represents an unstable environment in terms of communications (it is noise-sensitive and prone to failures). Therefore, the system should be tested before every implementation in the real

TABLE 10: Detection in 17-node network, scenario 1.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		0.0/0.0			0.0/0.0											
2	0.0/0.0		0.0/0.0			0.0/0.0										
3		0.0/0.0		0.0/0.0			0.0/0.0									
4			0.0/0.0					0.0/0.0								
5	0.0/0.0				0.0/0.0				0.0/0.0	80.3/80.3						
6		0.0/0.0				0.0/0.0					0.0/0.0					
7			0.0/0.0				0.0/0.0					0.0/0.0				
8				0.0/0.0				0.0/0.0					0.0/0.0			
9					0.0/0.0					80.3/80.3				0.0/80.3		
10						0.0/80.6			0.0/80.6		0.0/80.6				0.0/0.0	
11							0.0/0.0			80.3/80.3		0.0/0.0				0.0/0.0
12								0.0/0.0					0.0/0.0			0.0/0.0
13									0.0/0.0					0.0/0.0		
14										80.3/80.3					0.0/0.0	0.0/0.0
15											0.0/0.0					
16												0.0/0.0				
P_M (%)	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/0.0	0.0/20.2	0.0/0.0	0.0/0.0	0.0/26.9	<u>80.3/80.3</u>	0.0/20.2	0.0/0.0	0.0/0.0	0.0/26.8	0.0/0.0	0.0/0.0

TABLE II: Detection in 17-node network, scenario 2.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		0.0/0.0			0.0/0.0											
2	0.0/0.0		3.0/3.0			0.0/0.0										
3		0.0/0.0		5.9/5.9			1.5/1.5									
4			2.8/2.8					2.8/2.8								
5	0.0/0.0								1.5/1.5							
6		0.0/0.0			0.0/0.0		1.5/1.5			80.3/80.3						
7			2.9/2.9			0.0/0.0		2.9/2.9			1.5/1.5	7.2/7.2				
8				5.9/5.9			1.5/1.5						6.0/6.0			
9					0.0/0.0					79.1/79.1						
10						0.0/80.3			1.5/83.1		1.5/83.1			3.0/83.6	1.5/1.5	
11							1.5/1.5			79.1/79.1		7.4/7.4				7.0/7.0
12								2.8/2.8			1.4/1.4					
13									1.4/1.4				5.7/5.7	2.8/2.8	1.4/1.4	
14										75.4/75.4	1.5/1.5			2.9/2.9		7.5/7.5
15												6.9/6.9			1.4/1.4	
16											1.5/21.9	7.2/7.2	5.9/5.9	2.9/29.8	1.4/1.4	7.3/7.3
P_M (%)	0.0/0.0	0.0/0.0	2.9/2.9	5.9/5.9	0.0/0.0	0.0/20.1	1.5/1.5	2.8/2.8	1.5/28.7	<u>78.5/78.5</u>	1.5/21.9	7.2/7.2	5.9/5.9	2.9/29.8	1.4/1.4	7.3/7.3

TABLE 12: Detection in 17-node network, scenario 3.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		0.0/0.0			0.0/0.0											
2	3.1/3.1		12.1/12.1			0.0/0.0										
3		0.0/0.0		27.5/27.5			17.6/17.6									
4			8.3/8.3					24.7/24.7								
5	3.1/3.1					0.0/0.0			12.1/12.1							
6		0.0/0.0			0.0/0.0		20.0/20.0			80.3/80.3						
7			9.7/9.7			0.0/0.0		28.8/28.8			36.1/36.1					
8				20.1/20.1			12.0/12.0					48.0/48.0				
9					0.0/0.0					70.6/70.6			30.6/30.6			
10						0.0/80.3			9.0/83.3		33.5/90.3			23.6/86.4		
11							11.0/11.0			44.0/44.0		41.1/41.1			53.2/53.2	
12								9.0/9.0			11.3/11.3			20.7/20.7		24.2/24.2
13									7.9/7.9				23.8/23.8			
14										54.8/54.8				1.0/1.0	66.1/66.1	0.0/0.0
15											1.4/1.4				0.0/0.0	
16												2.3/2.3				
P_M (%)	3.1/3.1	0.0/0.0	10.0/10.0	23.8/23.8	0.0/0.0	0.0/20.1	15.2/15.2	20.8/20.8	9.7/34.4	<u>62.4/62.4</u>	20.6/34.8	30.5/30.5	27.2/27.2	15.1/36.0	39.8/39.8	12.1/12.1

network in order to adjust the probability threshold value to a particular application.

The number of neighbouring nodes is an important factor that influences the malevolence probability estimation process. Estimations of higher quality will be obtained in networks with a larger number of nodes, where malicious nodes have a larger number of legitimate neighbouring nodes. The estimations by legitimate nodes will in that case reduce a negative impact of false data inserted by a malicious node. Successful detection of malicious behaviour in a lossy environment (where the Rx/Tx success ratio is less than 100%) also depends on the chosen probability threshold value. A larger threshold value in a lossy environment lowers the detection efficacy since larger packet losses decrease the estimated malevolence probability for a malicious node and increase it for legitimate nodes. Also, if the threshold is too low, it is possible that a legitimate node will be characterized as malicious. The performed tests showed that many parameters influence the quality of estimation, for example, network topology (the number of nodes and their arrangement), the number of neighbours, packet loss (which is not caused by malicious behaviour), and a malicious node behaviour pattern. Therefore, it is not possible to define the universal probability threshold value that would be suitable for all networks.

7. Conclusions

In recent years, wireless sensor networks have been developing rapidly, and their application areas are extending continuously. Their strong resource limitations make them very specific and different from other types of wireless networks. Consequently, all usual networking mechanisms (e.g., routing or security mechanisms) required specific adaptations before their implementation into the WSN. Recently, there has been a strong tendency for interconnection of many different devices and integration of wireless sensor networks with other network types in the context of the Internet of Things paradigm. Protocol architecture of most current networks is based on the IP, and the transition to the new version of protocol (IPv6) is in progress. These parallel processes naturally led to the implementation of IPv6 into the WSN.

IPv6-based WSNs represent a novel trend in the area of sensor networks, and as such they raise certain problems and open issues that still require adequate solutions. Security aspects of IPv6-based WSNs are very important since good security solutions could guarantee their wider practical application. The paper gives an overview of security aspects of the IPv6-based WSN, focusing on existing security threats and different attack types. It also analyses some existing intrusion detection schemes that could be implemented into the IPv6-based WSN. The authors propose a solution for the distributed adaptive intrusion detection system intended especially for the IPv6-based WSN. Its distributed nature enables its execution on every sensor node in the network. Every node monitors the activity of its neighbours and estimates their malevolence probabilities. Final estimation of the malevolence probability for all nodes is calculated

after all IDS agents exchange their estimations. Calculation of the malevolence probability is also an advantage of the proposed intrusion detection system since most existing IDS just declare a certain node as malicious or legitimate, without estimation of the malevolence level.

The proposed system for malicious node detection fully supports the IPv6 in wireless sensor networks. As such, it is suitable for the IPv6-based WSN, while other intrusion detection solutions known from the conventional WSNs would require a proper adaptation (they cannot be directly applied into the IPv6-based WSN). Also, its advantage (compared to simple single-layer solutions) is possibility of integration into the unique cross-layer security framework along the other security mechanisms. Due to its distributed nature (where all network nodes contribute to decision-making process), the proposed system is tolerant on some node failures. The proposed system also estimates the malevolence probabilities for suspicious nodes, where most existing IDS do not estimate the malevolence level (they just declare node as a malicious or a legitimate one). Another advantage of the proposed system is adaptability for different application requirements achieved by the flexible (adjustable) malevolence threshold. At the same time, the proposed malicious node detection method proved to be energy efficient, which is very important in resource constrained environment of IPv6-based WSN. Finally, the proposed system showed very good detection capabilities despite lossy wireless environment and intentional aggravation of detection process by malicious nodes.

The proposed IDS solution was implemented in three different network topologies. In every network, detailed tests and analyses were performed through different characteristic scenarios. The goals of analysis were to examine performance and energy efficiency of the proposed IDS solution, its influence on normal network operation, and its capability of successful detection of malicious nodes in different situations. Successful detection is when the IDS correctly indicates a malicious node and extracts it from the set of legitimate nodes, giving thereby the malevolence probability estimation above the predefined threshold. The malicious node was deliberately inserted into the network for testing purposes. Therefore, it was surely possible to determine whether the IDS conclusion was correct or not. The tests performed also showed that the proposed IDS solution is energy efficient and with minor influence on normal network operation, while at the same time it has a very good capability of making correct decisions about malevolence of certain network nodes. In all testing scenarios, the IDS correctly indicated a malicious node, despite its attempts to falsely accuse its neighbours and to disable or at least aggravate the detection process. Future development of this IDS should include support for network node mobility that will additionally expand its possible application range.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.
- [2] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, 2007.
- [3] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.
- [4] RFC, "Internet protocol, version 6 (IPv6) specification," RFC 2460, 1998.
- [5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [6] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.
- [7] M. Blanchet, *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*, John Wiley & Sons, Chichester, UK, 2006.
- [8] K. Grgic and D. Zagar, "Wireless sensor networks-applications and development," in *Proceedings of the 2nd IFAC International Conference on Modelling and Design of Control Systems in Agriculture*, Osijek, Croatia, 2007.
- [9] J. Hui and P. Thubert, "Transmission of IPv6 packets over IEEE 802.15.4 networks," RFC 4944, IETF, 2007.
- [10] A. Dunkels and J. P. Vasseur, "IP for smart objects," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 1, 2008.
- [11] J. Abeille, M. Durvy, J. Hui, and S. Dawson-Haggerty, "Lightweight IPv6 stacks for smart objects: the experience of three independent and interoperable implementations," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 2, 2008.
- [12] K. Grgic, V. Krizanovic, and V. Mandric, "Security aspects of the RPL protocol implementation into IPv6-based wireless sensor networks," in *Proceedings of the 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM '14)*, Split, Croatia, 2014.
- [13] D. Žagar and K. Grgić, "IPv6 security threats and possible solutions," in *Proceedings of the World Automation Congress (WAC '06)*, pp. 1–7, IEEE, Budapest, Hungary, June 2006.
- [14] D. Žagar, K. Grgić, and S. Rimac-Drlje, "Security aspects in IPv6 networks—implementation and testing," *Computers & Electrical Engineering*, vol. 33, no. 5–6, pp. 425–437, 2007.
- [15] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.
- [16] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.
- [17] M. Saxena, "Security in wireless sensor networks—a layer-based classification," CERIAS Tech Report 04-2007, 2007.
- [18] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.
- [19] K. Stammberger, M. Semp, M. B. Anand, and D. Culler, "Introduction to security for smart object networks," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 5, 2010.
- [20] C. Krauß, M. Schneider, and C. Eckert, "On handling insider attacks in wireless sensor networks," *Information Security Technical Report*, vol. 13, no. 3, pp. 165–172, 2008.
- [21] A. Hamid, M. Rashid, and C. S. Hong, "Defense against laptop class attacker in wireless sensor network," in *Proceedings of the 8th International Conference Advanced Communication Technology (ICACT '06)*, pp. 314–318, Phoenix Park, Republic of Korea, February 2006.
- [22] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.
- [23] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.
- [24] V. P. Singh, S. Jain, and J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," *IJCSI International Journal of Computer Science Issues*, vol. 7, no. 11, pp. 23–27, 2010.
- [25] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Computer Communications*, vol. 30, no. 11–12, pp. 2353–2364, 2007.
- [26] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Algorithmic Aspects of Wireless Sensor Networks*, M. Kutylowski, J. Cichoń, and P. Kubiak, Eds., vol. 4837 of *Lecture Notes in Computer Science*, pp. 150–161, 2008.
- [27] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting Sybil attacks in wireless sensor networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042–3056, 2009.
- [28] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, pp. 1976–1986, San Francisco, Calif, USA, April 2003.
- [29] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless Ad Hoc networks," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48–60, 2004.
- [30] T. S. Sobh, "Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art," *Computer Standards & Interfaces*, vol. 28, no. 6, pp. 670–694, 2006.
- [31] F. Sabahi and A. Movaghar, "Intrusion detection: a survey," in *Proceedings of the 3rd International Conference on Systems and Networks Communications*, pp. 23–26, IEEE, Sliema, Malta, October 2008.
- [32] N. Marchang and R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," *Ad Hoc Networks*, vol. 6, no. 4, pp. 508–523, 2008.
- [33] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 56–63, 2007.
- [34] A. P. Lauf, R. A. Peters, and W. H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," *Ad Hoc Networks*, vol. 8, no. 3, pp. 253–266, 2010.
- [35] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006.
- [36] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks," in *Proceedings of the 6th European Conference on Wireless Sensor Networks (EWSN '09)*, pp. 263–278, Cork, Ireland, February 2009.

- [37] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05)*, pp. 253–259, Montreal, Canada, August 2005.
- [38] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698–711, 2008.
- [39] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.
- [40] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.
- [41] T. Chen, H. Huang, Z. Chen, Y. Wu, and H. Jiang, "A secure routing mechanism against wormhole attack in IPv6-based wireless sensor networks," in *Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Programming*, pp. 110–115, Nanjing, China, December 2015.
- [42] S. Lim and L. Huie, "Hop-by-Hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC '15)*, pp. 315–319, Garden Grove, Calif, USA, February 2015.
- [43] A. R. Dhakne and P. Chatur, "Distributed trust based intrusion detection approach in wireless sensor network," in *Proceedings of the Communication, Control and Intelligent Systems (CCIS '15)*, pp. 96–101, IEEE, Mathura, India, November 2015.
- [44] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.
- [45] C. B. Dutta and U. Biswas, "Specification based IDS for camouflaging wormhole attack in OLSR," in *Proceedings of the 23rd Mediterranean Conference on Control and Automation*, pp. 960–966, Torremolinos, Spain, June 2015.
- [46] Y. Mourabit, A. Bouriden, A. Toumanari, and N. Moussaid, "Intrusion detection techniques in wireless sensor network using data mining algorithms: comparative evaluation based on attacks detection," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 9, pp. 164–172, 2015.
- [47] J.-W. Ho, M. Wright, and S. K. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 512–523, 2012.
- [48] H. Moosavi and F. M. Bui, "A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1367–1379, 2014.
- [49] G. Sandhya and A. Julian, "Intrusion detection in wireless sensor network using genetic K-means algorithm," in *Proceedings of the IEEE International Conference on Advanced Communication, Control and Computing Technologies (ICACCCT '14)*, pp. 1791–1794, Ramanathapuram, India, May 2014.
- [50] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 3, pp. 256–269, 2015.
- [51] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718–3731, 2016.
- [52] C. Pu and S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation," *IEEE Systems Journal*, 2016.
- [53] K. Grgic, D. Zagar, and V. Krizanovic, "Security in IPv6-based wireless sensor network—precision agriculture example," in *Proceedings of the 12th International Conference on Telecommunications*, pp. 79–86, Zagreb, Croatia, June 2013.
- [54] T. Zia and A. Zomaya, "A security framework for wireless sensor networks," in *Proceedings of the IEEE Sensors Applications Symposium*, pp. 49–53, Houston, Tex, USA, February 2006.
- [55] N. R. Prasad and M. Alam, "Security framework for wireless sensor networks," *Wireless Personal Communications*, vol. 37, no. 3–4, pp. 455–469, 2006.
- [56] K. Sharma and M. K. Ghose, "Cross layer security framework for wireless sensor networks," *International Journal of Security and Its Applications*, vol. 5, no. 1, pp. 39–52, 2011.
- [57] A. Dunkels, B. Grönvall, and T. Voigt, "Contiki—a lightweight and flexible operating system for tiny networked sensors," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, pp. 455–462, Tampa, Fla, USA, November 2004.
- [58] F. Österlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with COOJA," in *Proceedings of the 1st IEEE Conference on Local Computer Networks*, pp. 641–648, IEEE, Tampa, Fla, USA, November 2006.
- [59] O. Gaddour and A. Koubâa, "RPL in a nutshell: a survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012.
- [60] J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: incorporating IEEE 802.15.4 into the IP architecture," IPSO Alliance (Internet Protocol for Smart Objects) Whitepaper 3, 2009.

